UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,885	09/16/2005	Claudine Viegas Conrado	NL 030293	7551

24737 7590 11/16/2010
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/549,885
Filing Date: September 16, 2005
Appellant(s): CONRADO ET AL.

Vincent K. Gustafson
Reg. No. 46,182
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 16, 2010 appealing from the Office action mailed March 16, 2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-10 and 12-31.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(**5) Summary of Claimed Subject Matter**

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading “WITHDRAWN REJECTIONS.” New grounds of rejection (if any) are provided under the subheading “NEW GROUNDS OF REJECTION.”

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant’s brief.

(8) Evidence Relied Upon

5,717,758	MICALL	2-1998
2007/0189542	ALLDREDGE	8-2007

Saito, T., "Privacy Enhanced Access Control by SPKI" Parallel and Distributed Systems: Workshops, Seventh International Conference on 4-7 July 2000 pp. 301-306.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1-2, 5-9, 12-19, 22-26, and 29-32 are rejected under 35 U.S.C. 103(a) as being obvious over Saito et al. (“Privacy Enhanced Access Control by SPKI”) in view of Micall (US 5,717,758).

Regarding Claims 1-2, 5, and 12-13:

Saito discloses a privacy enhanced access control by simple public key infrastructure that associates user identifying information (“An Identity” See page 301 section I.) and data (“Authorization Field of the SPKI Certificate” See pages 302-303) that conceals a user identity using concealing data (“Public Key of the subject in the SPKI certificate,” See pages 302-303 section II. B1.) in the user identifying information, wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), such that it is possible to check for a given user identity whether the association applies to it ("In a sense, this public key is a kind of disposable fingerprint: it isn't identical with ID, but it is a proof the client." See page 303 section II. C.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claims 6-8:

Saito discloses an issuing agent (See figure 5 ref. no. A) receives a request for an association from a client (See figure 5 ref. no. C) and the issuing agent provides an association signed by its own secret key to the client (See pages 304-305 Section III. B.).

Regarding Claim 14:

Saito discloses the privacy enhanced access control by simple public key infrastructure operates in internet and electronic commerce applications (See page 301 abstract). The examiner respectfully points out that pay per access content is available on the internet in electronic commerce applications.

Regarding Claim 15:

Saito discloses the authorization field of the SPKI Certificate has a content identifier (“File1, File2” See pages 302-303 section II. B1.)

Regarding Claim 16:

Saito discloses the SPKI Certificate includes a rights attributes data field (“Validity” See pages 302-303 section II. B1.).

Regarding Claims 18-19:

Saito discloses sending a request in relation to the data including the concealed user identifying information ("Exercise and Service communication between the Server and the Client" See figure 5 and page 305 section III. B.).

Regarding Claims 22-25:

Saito discloses privacy enhanced access control by simple public key infrastructure that receives from a user a request concerning the data using user identifying information related to the user (“SPKI S’ Certificate” and “SPKI A' Certificate” See figure 5 and pages 303-305 section III.), retrieves the association including user identifying information that has been concealed using concealing data ("Exercise" See pages 304-305 section III. B.) wherein the concealing data remains fixed for a set time period (“The validity field defines how the certificate is valid, for example a period of time.” See pages 302-303 section II. B1.), checks the concealed user identifying information in the association ("Exercise" See pages 304-305 section III. B.), and provides the user with information related to the data based on a correspondence between the concealed user identifying information in the association and the user identifying information at least linked to the user ("Exercise" and “Service” See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 26:

Saito discloses comparing the user identifying information of the user against a user domain certificate (“SPKI S' Certificate" See figure 5 and pages 304-305 section III. B.) including user identifying information related to all users in a domain (“The examiner respectfully points out that the amount of users in a domain can be as few as one.”), wherein the step of checking concealed user identifying information in the association with user identifying information is performed on user identifying information in the domain certificate (“SPKI S' Certificate" and “SPKI A' Certificate” See figure 5 and pages 304-305 section III. B.), and the step of providing is performed based on a correspondence between the concealed user identifying information in the association and any user identifying information in the domain certificate ("Secure Downloading" See pages 304-305 section III. B.).

Regarding Claim 29:

Saito discloses a privacy enhanced access control by simple public key infrastructure that conceals user identifying information ("An Identity" See page 301 section I.) in an association between a user and data ("Authorization Field of the SPKI Certificate" See pages 302-303) using concealing data ("Public Key of the subject in the SPKI certificate," See pages 302-303 section II. B1.) for provision of the concealed user identifying information in the association, wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.)

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 30:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives a request ("Exercise" See pages 304-305 section III. B.) from a user to access information in relation to an association between the user and, the data including user identifying information relating to the user (“SPKI A' Certificate” See figure 5 and pages 303-305 section III.), retrieve an association between the data and a user including user identifying information which has been concealed using concealing data (“Subject Field of the SPKI Certificate” and “Authorization Field of the SPKI Certificate" See pages 302-303 Section II.), wherein the concealing data remains fixed for a set time period (“The validity field defines how the certificate is valid, for example a period of time.” See pages 302-303 section II. B1.), check the concealed user identifying information in the association (“The server verifies the properness of certificates," See pages 304-305 section III. B.), provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user (“Secure Downloading” See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 31:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives user identifying information related to a user (“SPKI S’ Certificate” and “SPKI A' Certificate” See figure 5 and pages 303-305 section III.), the user identifying information being relation to an association between the user and data (“Authorization Field of the SPKI Certificate” See pages 302-303), identifying information is concealed using concealing data (“Public Key of the subject in the SPKI certificate,” See pages 302-303 section II. B1.), send a request concerning that data including the concealed user identifying information (“Exercise” See figure 5 ref. no. 4 and page 305), wherein the concealing data remains fixed for a set time period (“The validity field defines how the certificate is valid, for example a period of time.” See pages 302-303 section II. B1.), so that the association between the user and the data comprising the concealed user identifying information can be received (“The server verifies the properness of certificates," See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 32:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives a request (“Exercise” See figure 5 ref. no. 4 and page 305) concerning the data including the user identifying information which has been concealed using concealing data (“Public Key of the subject in the SPKI certificate,” See pages 302-303 section II. B1.), the data being included in an association between the user and the data (“Authorization Field of the SPKI Certificate” See pages 302-303), wherein the concealing data remains fixed for a set time period (“The validity field defines how the certificate is valid, for example a period of time.” See pages 302-303 section II. B1.), and provide the association between the user and the data comprising the concealed user identifying information (“The server verifies the properness of certificates," See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

2. Claims 3-4, 10, 20-21, 27-28 are rejected under 35 U.S.C. 103(a) as being obvious over Saito et al. (“Privacy Enhanced Access Control by SPKI”) in view of Micall (US 5,717,758) further in view of Alldredge (US 2007/0189542).

Regarding Claims 3 and 10:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure that conceals a user identity using a hash function.

Saito does not disclose concealing a user identity using encryption.

Alldredge discloses a cryptographic system that encrypts a users message using a symmetric key (See paragraph 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the privacy enhanced access control by simple public key infrastructure symmetric key based encryption such as that taught by Alldredge in order to achieve privacy between a message sender and a message receiver (See Alldredge paragraph 7).

Regarding Claim 4:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure that conceals a user identity using a hash function.

Saito does not disclose the concealing data includes a random value.

Alldredge discloses a method for secured electronic commerce using sequences of one time pads for concealing transmitted messages (See paragraphs 25 and 60)

It would have been obvious to one of ordinary skill in the art at the time of the invention to included in the privacy enhanced access control by simple public key infrastructure concealing transmitted messages using one time pads such as that taught by Alldredge in order to allow the privacy enhanced access control by simple public key infrastructure to be used internationally (See paragraph 19).

Regarding Claims 20-21 and 27-28:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure sending a request in relation to the data including the concealed user identifying information.

Saito does not disclose the request includes a secret security identifier and encrypting the concealing data using a secret domain key.

Alldredge discloses a cryptographic system that includes a secret security identifier (“Symmetric Key" See paragraphs 10 and 11) with a message and encrypts the message containing the secret security identifier using secret domain key ("Recipient's Public Key" See paragraphs 10 and 11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the privacy enhanced access control by simple public key infrastructure a symmetric key system and an asymmetric key system such as those taught by Alldredge in order to achieve privacy between a message sender and a message receiver (See Alldredge paragraph 7).

(10) Response to Argument

The Appellant argues:

That no basis or support exists for the hypothetical combination of Saito and Micall.

The Examiner contends that the Saito and Micall references are properly combinable. The Appellant argues that the use of Simple Public Key Infrastructure (SPKI) and Public Key Infrastructure (PKI) are not compatible. The Appellant argues that these two infrastructures as incompatible, and argues that PKI uses a certificate authority while SPKI does not require a certificate authority (Appeal Brief: page 10, paragraph 3). The Examiner contends that the Saito reference lays out the infrastructure, and that Micall was brought in only to teach that the authenticated deduced information includes at least one reissued certificate (Micall: column 1, lines 1-13) which indicates that a certificate is valid and/or indicating that the validity period of the certificate has been modified (Micall: column 1, lines 1-5). Therefore, the SPKI certificate of Saito will still have its user identity concealed (Saito: pages 302-303, section 11.B1) as the SPKI uses the public key as the subject of the SPKI certificate. Furthermore, the Examiner contends that since Micall was brought in only to teach the reissuing of valid certificates, it has to be this operation that has be evaluated in the infrastructure set forth by Saito. The Examiner points out that Saito does disclose the idea of re-issuing certificates (Saito: page 306, paragraph 7). Therefore, the Examiner contends that the method disclosed by Micall in reissuing valid certificates would be properly combinable since both infrastructures disclose the re-issuing of certificates. Under KSR International Co. V. Teleflex Inc., all that is required is that there is a rational underpinning for the obviousness. This rational underpinning requirement is clearly met as including reissuing SPKI certificates as taught in Micall would reduce overhead processing by reissuing a valid certificate instead of generating a new certificate. The Appellant argues that a third party re-issuing a certificate would change the principle of the operation of the art being modified (Appeal Brief: page 15, paragraph 4). The Examiner contends that Saito discloses that certificates are issued by an authorized server, which the client then uses to submit to service providers (Saito: see Abstract). Therefore, the Examiner contends that the authorized server could be in charge of the Micall operation of reissuing valid certificates without changing the principle operation of Saito, as the authorized server already exists in the Saito infrastructure (Saito: Abstract, Figure 2). Therefore, the Examiner contends that the combination of Saito and Micall is valid, and that the rejection of the independent claims is valid.

The Appellant finally contends that the Examiner conceded that Saito does not disclose reissuing associations between user identifying information and data, and argues that there is no proper basis to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure, therefore the limitations of the remaining claims are not disclosed by the combination of Saito and Micall. The Appellant refers to the arguments presented above which argue that Saito and Micall are not properly combinable. The Examiner contends that the Saito and Micall references are properly combinable. The Appellant argues that the use of Simple Public Key Infrastructure (SPKI) and Public Key Infrastructure (PKI) are not compatible. The Applicant argues that these two infrastructures as incompatible, and argues that PKI uses a certificate authority while SPKI does not require a certificate authority (Appeal Brief: page 10, paragraph 3). The Examiner contends that the Saito reference lays out the infrastructure, and that Micall was brought in only to teach that the authenticated deduced information includes at least one reissued certificate (Micall: column 1, lines 1-13) which indicates that a certificate is valid and/or indicating that the validity period of the certificate has been modified (Micall: column 1, lines 1-5). Therefore, the SPKI certificate of Saito will still have its user identity concealed (Saito: pages 302-303, section 11.B1) as the SPKI uses the public key as the subject of the SPKI certificate. Furthermore, the Examiner contends that since Micall was brought in only to teach the reissuing of valid certificates, it has to be this operation that is evaluated in the infrastructure set forth by Saito. The Examiner points out that Saito does disclose the idea of re-issuing certificates (Saito: page 306, paragraph 7). Therefore, the Examiner contends that the method disclosed by Micall in reissuing valid certificates would be properly combinable since both infrastructures disclose the re-issuing of certificates. Under KSR International Co. V. Teleflex Inc., all that is required is that there is a rational underpinning for the obviousness. This rational underpinning requirement is clearly met as including reissuing SPKI certificates as taught in Micall would reduce overhead processing by reissuing a valid certificate instead of generating a new certificate. The Appellant argues that a third party re-issuing a certificate would change the principle of the operation of the art being modified (Appeal Brief: page 15, paragraph 4). The Examiner contends that Saito discloses that certificates are issued by an authorized server, which the client then uses to submit to service providers (Saito: see Abstract). Therefore, the Examiner contends that the authorized server could be in charge of the Micall operation of reissuing valid certificates without changing the principle operation of Saito, as the authorized server already exists in the Saito infrastructure (Saito: Abstract, Figure 2). Therefore, the Examiner contends that the combination of Saito and Micall is valid, and that the rejection of the independent claims is valid.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Kaveh Abrishamkar/

Primary Examiner, Art Unit 2431

Conferees:

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431